

Латинские битрейды *

В. Н. Потапов

*Институт математики им. С. Л. Соболева СО РАН,
Новосибирский государственный университет, Новосибирск*

Аннотация

A subset S of k -ary n -dimensional hypercube is called latin bitrade if $|S \cap F| \in \{0, 2\}$ for each 1-face F . We find all admissible small (less than 2^{n+1}) cardinalities of latin bitrades.

A subset M of k -ary n -dimensional hypercube is called t -fold MDS code if $|M \cap F| = t$ for each 1-face F . Symmetric difference of two 1-fold MDS codes is always a latin bitrade. Symmetric difference of two t -fold MDS codes may also be a latin bitrade. In this case we say that latin bitrade embedded into t -fold MDS code. The intersection of t -fold MDS code and a latin bitrade embedded into it is called a component of the code. We study the questions of embedding of latin bitrades into t -fold MDS and admissible cardinalities of the component of t -fold MDS.

Key words: MDS code, latin bitrade, component.

Аннотация

Подмножество k -значного n -мерного гиперкуба называется латинским битрейдом если мощности его пересечений с одномерными гранями гиперкуба принимают только два значения 0 и 2. Найдены все возможные меньшие 2^{n+1} числа, которые являются мощностями некоторых латинских битрейдов.

Подмножество k -значного n -мерного гиперкуба называется t -кратным МДР-кодом, если оно пересекается с каждой одномерной гранью гиперкуба ровно по t элементам. Симметрическая разность двух однократных МДР-кодов является латинским битрейдом. Полученные таким образом битрейды называются вложимыми в МДР-код, а пересечение битрейда с каждым из двух МДР-кодов называется компонентой МДР-кода. В статье исследованы вопросы о вложимости латинских битрейдов в МДР-коды и о возможных мощностях компонент кодов.

Ключевые слова: МДР-код, латинский битрейд, компонента.

§ 1. Определения

Пусть $Q_k = \{0, 1, \dots, k-1\}$. Обозначим через Q_k^n множество упорядоченных k -ичных наборов (вершин) длины n . Расстоянием Хэмминга $d(x, y)$ между вершинами $x, y \in Q_k^n$ называется число позиций, в которых наборы x и y различаются. Через ΓQ_k^n обозначим граф минимальных расстояний метрического пространства (Q_k^n, d) . Гранью размерности k называется подмножество гиперкуба Q_k^n , состоящее из вершин с одинаковыми фиксированными значениями некоторых $n-k$ координат. В частности, одномерная грань направления i , проходящая через вершину $(a_1, \dots, a_n) \in Q_k^n$, определяется как множество $\{(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) \mid x \in Q_k\}$.

*Работа выполнена при поддержке Российского фонда фундаментальных исследований (проекты 10-01-00424, 10-01-00616) и ФЦП <Научные и научно-педагогические кадры инновационной России> на 2009-2013 гг. (гос. контракт № 02.740.11.0429)

МДР-кодом (с расстоянием 2) называется множество $M \subset Q_k^n$ пересекающееся с каждой одномерной гранью ровно по одному элементу. Нетрудно видеть, что множество $M \subset Q_k^n$ является МДР-кодом тогда и только тогда, когда оно имеет мощность k^{n-1} и расстояние между любыми двумя различными элементами из M не менее двух. Множество W называется t -кратным МДР-кодом, если оно пересекается с каждой одномерной гранью ровно по t элементам. t -Кратный МДР-код называется *расщепляемым*, если он является объединением t однократных МДР-кодов. Кратные нерасщепляемые МДР-коды рассматриваются в [1]. Понятие кратного МДР-кода с расстоянием d совпадает с понятием корреляционно-иммунной функции порядка $n - d + 1$ в Q_k^n .

Множество $B \subset Q_k^n$ называется *латинским битрейдом*, если мощности его пересечений с одномерными гранями принимают только два значения 0 и 2. Латинский битрейд $B \subset Q_k^n$ будем называть *двудольным*, если подграф графа ΓQ_k^n порождённый множеством вершин B является двудольным. Ясно, что симметрическая разность двух МДР-кодов является двудольным битрейдом. Латинский битрейд B будем называть *вложимым* в МДР-код M_1 (возможно кратный), если найдётся такой МДР-код M_2 (той же кратности), что $B = M_1 \Delta M_2$. В этом случае множество $B \cap M_1$ называется *компонентой* МДР-кода M_1 .

§ 2. Битрейды

Следующие два утверждения доказаны в [4] при $k = 4$, однако доказательство при произвольном $k \geq 2$ точно такое же.

Предложение 1. Пусть $B \subset Q_k^n$ латинский битрейд, тогда $|B| \geq 2^n$.

Предложение 2. Пусть $B \subset Q_k^n$ латинский битрейд. Следующие условия эквивалентны:

- a) $|B| = 2^n$,
- b) для любой m -мерной грани мощность её пересечения с B равняется 0 или 2^m ,
- c) B пересекается только с двумя гипергранями каждого направления,
- d) подграф графа ΓQ_k^n порождённый множеством B изоморфен булеву кубу ΓQ_2^n .

Из предложения 1 непосредственно вытекает, что в Q_2^n существует единственный битрейд, совпадающий со всем множеством Q_2^n . Вычислим число битрейдов в Q_3^n .

Предложение 3. В гиперкубе Q_3^n имеется ровно 2^{2^n} различных латинских битрейдов.

Доказательство. Рассмотрим произвольное подмножество $A \subseteq \{0, 1\}^n \subset Q_3^n$. Покажем, что существует такой битрейд $B \subset Q_3^n$, что $B \cap \{0, 1\}^n = A$. Определим частичный порядок на Q_3 : $0 < 2$, $1 < 2$, а символы 0 и 1 несравнимы. Пусть $(x_1, \dots, x_n) \in \{0, 1\}^n$ и $(y_1, \dots, y_n) \in Q_3^n \setminus \{0, 1\}^n$. Введём обозначение $(x_1, \dots, x_n) < (y_1, \dots, y_n)$, если для любого $i = 1, \dots, n$ верно, что $x_i < y_i$ или $x_i = y_i$. Определим функцию $f : Q_3^n \rightarrow \{0, 1\}$ равенством

$$f(y) = \begin{cases} \chi^A(y) & \text{при } y \in \{0, 1\}^n, \\ \bigoplus_{x < y} \chi^A(x) & \text{при } y \notin \{0, 1\}^n, \end{cases}$$

где χ^A — характеристическая функция множества A . Из определения имеем равенство

$$f(a_1, \dots, a_{i-1}, 2, a_{i+1}, \dots, a_n) = f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \oplus f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$$

для любых $a_j \in Q_3$. Тогда f — характеристическая функция некоторого битрейда $B \subset Q_3^n$. Очевидно, что характеристическая функция битрейда в Q_3^n полностью определяется своим сужением на $\{0, 1\}^n$ и множество подмножеств булева n -куба $\{0, 1\}^n$ имеет мощность 2^{2^n} .

▲

Отметим, что в соответствии с определением булева функция $f|_{\{0,2\}^n}$ является преобразованием Мёбиуса от функции χ^A .

При $k \geq 4$ число и даже асимптотика логарифма числа латинских битрейдов остаются неизвестными. Остаётся открытым вопрос о числе двудольных битрейдов в Q_k^n при $k \geq 3$. Более подробно вопрос о числе битрейдов в Q_k^n и его связь с другими комбинаторными задачами обсуждается в [6].

Следующее предложение обеспечивает конструктивный способ построения битрейдов.

Предложение 4.

- а) Декартово произведение двух латинских битрейдов является латинским битрейдом;
- б) декартово произведение двух двудольных битрейдов является двудольным битрейдом.

Доказательство пункта (а) непосредственно вытекает из определений, при доказательстве пункта (б) пользуемся тем, что декартово произведение двудольных графов является двудольным графом.

Предложение 5.

- а) Симметрическая разность (при $k=3$) двух латинских битрейдов является латинским битрейдом;
- б) если симметрическая разность двух двудольных битрейдов является битрейдом, а их пересечение порождает связный подграф в гиперкубе, то симметрическая разность является двудольным битрейдом.

Доказательство пункта (а) непосредственно вытекает из определений, при доказательстве пункта (б) пользуемся тем, что связный двудольный граф однозначно разделяется на доли.

Предложение 6. Пусть $B \subset Q_k^n$ латинский битрейд и $2^{n+1} > |B| \geq 2^n$. Тогда $|B| = 2^{n+1} - 2^s$, где $s \in \{1, \dots, n\}$.

Доказательство. Будем доказывать утверждение методом индукции по n . При $n = 1$ утверждение очевидно, предположим оно верно при $n - 1$. Если латинский битрейд $B \subset Q_k^n$ содержится в объединении двух гиперграней каждого направления, то по предположению 2 $|B| = 2^n$.

Пусть латинский битрейд B пересекается с тремя гипергранями одного направления. Если пересечение хотя бы с одной из них имеет мощность большую либо равную 2^n , то по предположению 1 имеем $|B| \geq 2^{n+1}$. В противном случае по предположению индукции имеем $|B| = 3 \cdot 2^n - 2^{s_1} - 2^{s_2} - 2^{s_3}$. Поскольку неравенство $2^{s_1} + 2^{s_2} + 2^{s_3} > 2^n$ выполнено только когда как минимум два из трёх s_i равняются $n - 1$, то имеем $|B| = 2^{n+1} - 2^s$. ▲

Предложение 7. Для любого $s \in \{0, \dots, n - 1\}$ существует двудольный битрейд $B_s \subset Q_3^n$ такой, что $|B_s| = 2^{n+1} - 2^{s+1}$.

Доказательство. Из предложений 4 и 5 следует, что множество $B_s = (\{0, 1\}^{n-s} \triangle \{1, 2\}^{n-s}) \times \{0, 1\}^s$ является двудольным битрейдом. Очевидно $|B| = 2^s(2^{n-s} + 2^{n-s} - 2)$. ▲

§ 3. МДР-коды

Известно (см, например, [2]), что все МДР-коды в гиперкубе Q_3^n эквивалентны при каждом $n \geq 1$. Характеризация всех МДР-кодов в гиперкубе Q_4^n имеется в [5]. Как было указано

выше, симметрическая разность $M_1 \Delta M_2$ двух МДР-кодов M_1 и M_2 является битрейдом вложимым в эти МДР-коды. Нетрудно видеть, что вложимые МДР-коды являются двудольными, причём каждая из долей $M_1 \cap (M_1 \Delta M_2)$ $M_2 \cap (M_1 \Delta M_2)$ является компонентой соответствующего МДР-кода. Таким образом в предложении 6 получены ограничения на возможные мощности компонент МДР-кодов. Ниже рассмотрен вопрос о вложимости битрейдов в МДР-коды (в том числе кратные).

Для произвольной функции $f : Q_k^n \rightarrow Q_k$ обозначим её график через $\mathcal{M}\langle f \rangle = \{(\bar{x}, f(\bar{x})) : \bar{x} \in Q_k^n\}$. Если множество $\mathcal{M}\langle f \rangle$ является МДР-кодом, то функция f называется n -арной квазигруппой порядка k . Соответственно, частичной n -арной квазигруппой порядка k называется функция, график которой пересекается с любой одномерной гранью не более чем по одной вершине.

В [3] доказано, что любая частичная n -арная квазигруппа конечного порядка вложима в n -арную квазигруппу некоторого большего порядка. Отсюда нетрудно получить

Предложение 8. Любой двудольный латинский битрейд $B \subset Q_k^n$ вложим в некоторый МДР-код $M \subset Q_m^n$, где $m \geq k$.

Предложение 9. Латинский битрейд $B \subset Q_k^n$ такой, что $2^{n+1} > |B| > 2^n$, не вложим в МДР-коды $M \subset Q_k^n$ при $k = 3$ и $k = 4$.

Д О К А З А Т Е Л Ъ С Т В О . Поскольку все МДР-коды в Q_3^n эквивалентны при любом n , достаточно рассмотреть произвольный МДР-код в Q_3^n , например, $M = \{x \in Q_3^n \mid x_1 + \dots + x_n = 0 \bmod 3\}$. Нетрудно видеть, что любой вложимый в M битрейд содержит весь МДР-код M и имеет мощность $2 \cdot 3^{n-1}$.

Пусть $k = 4$. Рассмотрим трёхмерные вложимые битрейды. Полным перебором нетрудно убедиться, что если вложимый в МДР-код $M \subseteq Q_4^3$ битрейд B имеет пересечение мощности не менее 6 с некоторой двумерной гранью, то найдётся ещё одна двумерная грань параллельная первой, пересечение с которой также имеет мощность не менее 6. Кроме того, полным перебором можно проверить, что в этом случае $|B| \geq 16 = 2^4$. Тогда, применяя метод индукции получаем, что если вложимый битрейд $B' \subseteq Q_4^n$ имеет пересечение мощности не менее 6 с какой-либо двумерной гранью, то $|B'| \geq 2^{n+1}$. Из предложения 10 следует, что если пересечение латинского битрейда с любой двумерной гранью имеет мощность меньше 6, т. е. равную 0 или 4, то граф порождённый битрейдом B' является булевым n -кубом. \blacktriangle

Пусть C — множество двухэлементных подмножеств в Q_4 , $|C| = 6$. Пусть $c \in C$, введём обозначение $\bar{c} = Q_4 \setminus c$. Каждая функция $g : Q_4^n \rightarrow C$ взаимно однозначно соответствует множеству $F(g) \subset Q_4^{n+1}$, определённого равенством $F(g) = \{(a_1, \dots, a_n, a) \mid a \in g(a_1, \dots, a_n)\}$.

Нетрудно видеть, что справедливо следующее

Предложение 10. Множество $F(g) \subset Q_4^{n+1}$ является двукратным МДР-кодом тогда и только тогда, когда для любого $c \in C$ и любой одномерной грани функция g принимает в ней значения c и \bar{c} одинаковое число раз.

Предложение 11. Для любого $s \in \{1, \dots, n\}$ существует вложимый в двукратный МДР-код $M \subset Q_4^n$ латинский битрейд $B \subset Q_4^n$ такой, что $|B| = 2^{n+1} - 2^s$.

Д О К А З А Т Е Л Ъ С Т В О . Введём обозначения $\alpha = \{0, 2\}$, $\beta = \{1, 2\}$. Определим функции

$$g(a_1, \dots, a_n) = \begin{cases} \alpha & \text{при } \sum_{i=1}^n a_i = 0 \bmod 2, \\ \bar{\alpha} & \text{при } \sum_{i=1}^n a_i = 1 \bmod 2; \end{cases}$$

$$g'(a_1, \dots, a_n) = \begin{cases} \alpha & \text{при } g(a_1, \dots, a_n) = \alpha, (a_1, \dots, a_n) \notin \{1, 2\}^n, \\ \alpha & \text{при } g(a_1, \dots, a_n) = \bar{\alpha}, (a_1, \dots, a_n) \in \{1, 2\}^n, \\ \bar{\alpha} & \text{при } g(a_1, \dots, a_n) = \bar{\alpha}, (a_1, \dots, a_n) \notin \{1, 2\}^n, \\ \bar{\alpha} & \text{при } g(a_1, \dots, a_n) = \alpha, (a_1, \dots, a_n) \in \{1, 2\}^n; \end{cases}$$

$$h_s(a_1, \dots, a_n) = \begin{cases} g'(a_1, \dots, a_n) & \text{при } (a_1, \dots, a_n) \notin B_s, \\ \beta & \text{при } (a_1, \dots, a_n) \in B_s, g'(a_1, \dots, a_n) = \alpha, \\ \bar{\beta} & \text{при } (a_1, \dots, a_n) \in B_s, g'(a_1, \dots, a_n) = \bar{\alpha}. \end{cases}$$

Из предложения 10 следует, что множества $F(g)$ и $F(g')$ являются двукратными МДР-кодами. Из предложений 7 и 10 получаем, что множество $F(h_s)$ является двукратным МДР-кодом. Нетрудно видеть, что $F(g') \triangle F(h_s) = B_s$. ▲

Приведём таблицы функций g, g', h_1 при $n = 2$

$$\begin{pmatrix} \alpha & \bar{\alpha} & \alpha & \bar{\alpha} \\ \bar{\alpha} & \alpha & \bar{\alpha} & \alpha \\ \alpha & \bar{\alpha} & \alpha & \bar{\alpha} \\ \bar{\alpha} & \alpha & \bar{\alpha} & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \bar{\alpha} & \alpha & \bar{\alpha} \\ \bar{\alpha} & \bar{\alpha} & \alpha & \alpha \\ \alpha & \alpha & \bar{\alpha} & \bar{\alpha} \\ \bar{\alpha} & \alpha & \bar{\alpha} & \alpha \end{pmatrix}, \begin{pmatrix} \beta & \bar{\beta} & \alpha & \bar{\alpha} \\ \bar{\beta} & \bar{\alpha} & \beta & \alpha \\ \alpha & \beta & \bar{\beta} & \bar{\alpha} \\ \bar{\alpha} & \alpha & \bar{\alpha} & \alpha \end{pmatrix}.$$

Можно показать, что построенные в предложении 11 двукратные МДР-коды $F(h_s)$ являются нерасщепляемыми.

Список литературы

1. Кротов Д.С., Потапов В.Н. О кратных МДР- и совершенных кодах, не расщепляемых на однократные // Проблемы передачи информации, 2004. Т. 40, N 1. С. 6-14.
2. Потапов В.Н., Кротов Д.С. Асимптотика числа n -квазигрупп порядка 4 // Сиб. мат. журн. 2006. Т. 47, №4. С. 873–887.
3. Cruse A.B. On the finite completion of partial latin cube // J. of Combinatorial Theory (A), 1974. V. 17. P. 112–119.
4. Krotov D.S. On decomposability of 4-ary distance 2 MDS codes, double-codes, and n -quasigroups of order 4 // Discrete Math., 2008. V. 308, N 15. P. 3322–3334.
5. Krotov D.S., Potapov V.N. n -Ary quasigroups of order 4 // SIAM J. Discrete Math. 2009. V. 23, N 2. P. 561-570.
6. Krotov D.S., Potapov V.N. On the number of n -ary quasigroups of finite order // Дискретная математика. 2011. (принята в печать)